

### **IN THE CLAIMS**

Please amend the claims as follows:

1. (Currently Amended) A method for detecting fraud by a payment facilitator when facilitating a payment transaction over a global wide area network, the method comprising:

receiving, by the payment facilitator via a web site interface, sale information pertaining to a purchase of a product from a seller, wherein the sale information includes an email address for the seller;

receiving, by the payment facilitator via the web site interface, payment information from a buyer, where the payment information includes an email address for the buyer, and wherein the payment information is received from the buyer in response to an email generated invoice sent to the email address of the buyer or sent in response to an email generated notification of a location that the buyer can acquire the email generated invoice where the location is sent to the email address of the buyer;

performing, by the payment facilitator, automated analysis of transaction information including the sale information and the payment information to detect whether the transaction information indicates fraud, and wherein the payment facilitator executes a software program to process at least some information associated with historical information, in order to determine whether fraud is present;

if the automated analysis does not detect fraud, the payment facilitator sends information via email to the email address of the seller instructing the seller to send the product to the buyer, credits an account of the seller for the purchase in response to an indication that the buyer received the product, and the payment facilitator directly contacts a financial institution associated with the buyer, via a dedicated line, and debits another account associated with the buyer at that financial institution; and

if the automated analysis detects fraud, the payment facilitator causes an enhanced transaction information to be communicated to a human for manual fraud analysis.

2. (Original) The method of Claim 1 wherein the sale information is received from a seller, and the method further comprises:  
communicating an invoice to a buyer.
3. (Cancelled)
4. (Original) The method of Claim 1 further comprising:  
performing simple screening of the transaction information.
5. (Original) The method of Claim 4 wherein performing simple screening comprises at least one of:  
determining whether a financial account specified as part of the payment information is on a list of known fraudulent financial account numbers;  
determining whether the name of the buyer or the name of the seller is on a list of known fraudulent users;  
determining whether a shipping address specified as part of the payment information is on a list of known fraudulent addresses;  
determining whether a billing address specified as part of the payment information is on a list of known fraudulent addresses;  
determining whether a billing address specified as part of the payment information is on a list of known fraudulent addresses;  
determining whether an email address of the buyer or the seller is on a list of known fraudulent email addresses; and  
determining whether an Internet protocol (IP) address of the buyer or the seller is on a list of known fraudulent IP addresses.
6. (Previously Presented) The method of Claim 1 further comprising:  
seeking approval from the financial institution based on the payment information.

7. (Original) The method of Claim 6 wherein seeking approval comprises:  
    sending a request for approval that comprises at least an account information extracted from the payment information and an amount information to a financial institution;  
    receiving from the financial institution a response to the request;  
rejecting the payment transaction or continuing with the payment transaction responsive to the response.
8. (Original) The method of Claim 1 wherein performing automated analysis comprises:  
    performing rule-based analyses.
9. (Original) The method of Claim 8 wherein performing rule-based analyses comprises:  
    applying a plurality of rules to the transaction information such that a score for the payment transaction is incremented when one of the rules is violated.
10. (Original) The method of Claim 9 wherein performing rule-based analyses further comprises:  
    creating the enhanced transaction information if the score exceeds a predefined threshold such that the enhanced transaction information comprises a tracking number, the score, and a violated rule information.
11. (Original) The method of Claim 9 wherein applying comprises:  
    incrementing the score responsive to a numeric value assigned to the rule violated.
12. (Original) The method of Claim 9 wherein the plurality of rules comprise at least one of a plurality of suspect data rules and a plurality of velocity rules.

13. (Original) The method of Claim 12 wherein the plurality of suspect data rules comprise at least some of:

- comparison of a shipping address with a directory of known real addresses;
- comparison of a shipping address with a list of addresses implicated in prior possibly fraudulent transactions;
- comparison of a billing address with a directory of known real addresses;
- comparison of a billing address with a list of addresses implicated in prior possibly fraudulent transactions.

14. (Original) The method of Claim 12 wherein the plurality of velocity rules comprise at least some of:

- determining whether a first number of transactions involving the seller exceeds a first predefined threshold for a first predefined time period;
- determining whether a second number of transactions involving the buyer exceeds a second predefined threshold for a second predefined time period;
- determining whether a first total dollar amount for a first plurality of transactions involving the buyer exceeds a third predefined threshold for a third predefined time period;
- determining whether a second total dollar amount for a second plurality of transactions involving the seller exceeds a fourth predefined threshold for a fourth predefined time period;
- determining whether a third total dollar amount for a specified financial account exceeds a fifth predefined threshold for a fifth predefined time period;
- determining whether a third number of transactions involving the specified financial account exceeds a sixth predefined threshold for a sixth predefined time period.

15. (Previously Presented) The method of Claim 12 wherein the plurality of velocity rules comprise at least some of:

determining whether a financial account specified as part of the payment information has exceeded a predetermined acceptable number of times used over a predetermined period of time;

determining whether a financial account specified as part of the payment information has exceeded a predetermined acceptable number of times used over a predetermined number of transactions with the seller;

determining whether a financial account specified as part of the payment information has exceeded a predetermined acceptable number of times used over a predetermined number of transactions with the payment facilitator.

16. (Original) The method of Claim 1 wherein communicating an enhanced transaction information comprises sending an email message to at least one of a plurality of human fraud investigators.

17. (Original) The method of Claim 1 further comprising:

if the analyzing indicates fraud, notifying the buyer and/or a seller that the payment transaction is on hold pending the outcome of a fraud investigation.

18. (Original) The method of Claim 17 wherein notifying comprises:

sending an email message to the buyer and/or the seller.

19. (Currently Amended) A system comprising:

a first computer supporting communications over a wide area network by a buyer,  
wherein the communications over the wide area network occur via a web site interface for a payment facilitator;

a second computer supporting communications over the wide are network by a seller,  
wherein the communications over the wide area network occur via the web site interface for the payment facilitator;

the [[a]] payment facilitator computer supporting communications over the wide are network and executing software that facilitates a payment transaction between the buyer and the seller such that the payment facilitator computer

analyzes the payment transaction for fraud by applying a plurality of rules and incrementing a score for the payment transaction for each of the plurality of rules that is violated,

if the score does not exceed a predefined threshold, instructs the seller via email to send a purchased product to the buyer, credits an account of the seller for the payment transaction in response to an email indication that the buyer received the purchased product, and the payment facilitator directly contacts a financial institution associated with the buyer, via a dedicated line, and debits another account associated with the buyer at that financial institution, and

if the score exceeds a predefined threshold, communicates an information about the payment transaction to a human fraud investigator, and wherein a number of the rules are applied in response to information related to historical information that compliments the rules.

20. (Original) The system of Claim 19 further comprising:

a fourth computer capable of communications with the third computer and allowing the human fraud investigator to communicate with the third computer.

21. (Original) The system of Claim 20 wherein the third computer is coupled to the fourth computer via a dedicated communications line.
22. (Original) The system of Claim 20 wherein the third computer communicates with the fourth computer over the wide area network.
23. (Previously Presented) The system of Claim 19 further comprising:  
a fifth computer capable of communications with the third computer and responding on behalf of the financial institution to a request for authorization of the payment transaction initiated by the software executing on the third computer.
24. (Original) The system of Claim 23 wherein the third computer is coupled to the fifth computer via a dedicated communications line.
25. (Original) The system of Claim 23 wherein the third computer communicates with the fifth computer over the wide area network.
26. (Original) The system of Claim 19 wherein the wide area network is the Internet.
27. (Currently Amended) A machine readable medium having stored thereon instructions which when executed by a processor cause the machine to perform a method for detecting fraud by a payment facilitator when facilitating a payment transaction over a global wide area network, the method comprising:  
receiving, via a web site interface of the payment facilitator, sale information pertaining to a purchase of a product from a seller, and wherein the sale information includes an email address for the seller;  
receiving, via the web site interface of the payment facilitator, payment information from a buyer, and wherein the payment information includes an email address for the buyer;  
performing, by the payment facilitator, automated analysis of transaction information including the sale information and the payment information to detect whether

the transaction information indicates fraud, and wherein the payment facilitator acquires at least some information related to historical information, in order to determine if fraud is present;

if the automated analysis does not detect fraud, the payment facilitator sends information via email instructing the seller to send the product to the buyer, credits an account of the seller for the purchase in response to an email indication that the buyer received the product, and the payment facilitator directly contacts a financial institution associated with the buyer, via a dedicated line, and debits another account associated with the buyer at that financial institution; and

if the automated analysis detects fraud, the payment facilitator causes an enhanced transaction information to be communicated to a human for manual fraud analysis.

28. (Original) The machine readable medium of Claim 27 wherein the instructions cause the machine to perform operations further comprising:

performing simple screening of the transaction information.

29. (Original) The machine readable medium of Claim 28 wherein performing simple screening comprises at least one of:

determining whether a financial account specified as part of the payment information is on a list of known fraudulent financial account numbers;

determining whether the name of the buyer or the name of the seller is on a list of known fraudulent users;

determining whether a shipping address specified as part of the payment information is on a list of known fraudulent addresses;

determining whether a billing address specified as part of the payment information is on a list of known fraudulent addresses;

determining whether a billing address specified as part of the payment information is on a list of known fraudulent addresses;

determining whether an email address of the buyer or the seller is on a list of known fraudulent email addresses; and



determining whether an Internet protocol (IP) address of the buyer or the seller is on a list of known fraudulent IP addresses.

30. (Previously Presented) The machine readable medium of Claim 27 wherein the instructions cause the machine to perform operations further comprising:  
seeking approval from the financial institution based on the payment information.

31. (Original) The machine readable medium of Claim 30 wherein seeking approval comprises:  
sending a request for approval that comprises at least an account information extracted from the payment information and an amount information to a financial institution;  
receiving from the financial institution a response to the request;  
rejecting the payment transaction or continuing with the payment transaction responsive to the response.

32. (Original) The machine readable medium of Claim 27 wherein performing automated analysis comprises:  
performing rule-based analyses.

33. (Original) The machine readable medium of Claim 32 wherein performing rule-based analyses comprises:  
applying a plurality of rules to the transaction information such that a score for the payment transaction is incremented when one of the rules is violated.

34. (Original) The machine readable medium of Claim 33 wherein performing rule-based analyses further comprises:  
creating the enhanced transaction information if the score exceeds a predefined threshold such that the enhanced transaction information comprises a tracking number, the score, and a violated rule information.

35. (Original) The machine readable medium of Claim 33 wherein applying comprises:  
incrementing the score responsive to a numeric value assigned to the rule violated.
36. (Original) The machine readable medium of Claim 33 wherein the plurality of rules  
comprise at least one of a plurality of suspect data rules and a plurality of velocity rules.
37. (Original) The machine readable medium of Claim 27 wherein communicating an  
enhanced transaction information comprises sending an email message to at least one of a  
plurality of human fraud investigators.
38. (Original) The machine readable medium of Claim 27 wherein the instructions cause the  
machine to perform operations further comprising:  
if the analyzing indicates fraud, notifying the buyer and/or a seller that the payment  
transaction is on hold pending the outcome of a fraud investigation.
39. (Original) The machine readable medium of Claim 38 wherein notifying comprises:  
sending an email message to the buyer and/or the seller.